Pwnie Express User Manual

Mobile Product Line

Pwn Pad 3

(NVIDIA SHIELD)

The latest version of this manual is maintained here:
http://www.pwnieexpress.com/pages/documentation

Table of Contents

Legal Disclaimers

- All Pwnie Express products are for legally authorized use only.
- By using this product you agree to the terms of the Rapid Focus Security, Inc. EULA: (http://www.pwnieexpress.com/wp-content/uploads/2014/12/Pwnie-Express-EULA-10-13-14-.pdf)
- This product contains both open source and proprietary software:
    - Proprietary software is distributed under the terms of the Rapid Focus Security, Inc. EULA: (http://www.pwnieexpress.com/wp-content/uploads/2014/12/Pwnie-Express-EULA-10-13-14-.pdf)
    - Open source software is distributed under one or more of the following licenses:
        - GNU PUBLIC LICENSE (https://www.gnu.org/licenses/gpl.html)
        - BSD-3-CLAUSE LICENSE (http://opensource.org/LICENSES/BSD-3-CLAUSE)
        - OPENSSL TOOLKIT DUAL LICENSE (https://www.openssl.org/source/license.html)
        - APACHE LICENSE, VERSION 2.0 (https://www.apache.org/licenses/LICENSE-2.0.html)
- As with any software application, any downloads/transfers of this software are subject to export controls under the U.S. Commerce Department's Export Administration Regulations (EAR): (http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear). By using this software, you certify your complete understanding of and compliance with these regulations.

Specifications

Hardware

• PROCESSOR	NVIDIA® Tegra® K1 192 core Kepler GPU 2.2 GHz ARM Cortex A15 CPU with 2GB RAM
• DISPLAY	8-inch 1920x1200 multi-touch Full HD display
• AUDIO	Front facing stereo speakers, dual bass reflex port with built-in mic
• STORAGE	32 GB (WiFi+4G LTE)
• INTERFACE	Mini-HDMI output Micro-USB 2.0 MicroSD storage slot 3.5 mm stereo headphone jack with microphone support
• SIM CARD	Micro-SIM
• CAMERAS	Front: 5MP HDR; Back: 5MP auto focus HDR
• BATTERY	19.75 Watt Hours
• WEIGHT AND SIZE	Weight: 13.7oz / 390g Height: 8.8in / 221mm Width: 5.0in / 126mm, Depth: 0.36in / 9.2mm
• OPERATING SYSTEM	Android 4.4.2 KitKat

Wireless

- WIRELESS (built-in) 802.11n 2x2 Mimo 2.4 GHz and 5 GHz Wi-Fi
  Bluetooth 4.0 LE
  GPS / GLONASS

Cellular

- CONNECTIVITY North America: Unlocked LTE, HSPA+, 3G, 2G, GSM, EDGE
  Outside-North America: Unlocked LTE, HSPA+, 3G, 2G, GSM, EDGE
- CELLULAR BANDS North America:
  LTE: Bands 2,4,5,7,17 (1900, 1700, 850, 2600, 700)
  HSPA+: Bands 1,2,4,5 (2100, 1900, 1700, 850)
  Outside-North America:
  LTE: Bands 1*,3,7,20 (2100/1800/2600/800)
  HSPA+: Bands 1,2,5,8 (2100/1900/850/900)

Getting Started

Things to be aware of

- The Pwnie Express mobile product line is designed exclusively for conducting wired and wireless network security assessments. Using this product as a personal mobile device is **not** recommended, or supported.
- Google Play Services, including Google Play Store are **not** installed by default on the Pwn Pad 3. To install, please see the section entitled "*Update Notifications*".
- Do **not** use the Factory Data Reset feature available within Android Settings. Doing so will cause the Pwn Pad to revert to a stock Android 4.4.2 image, additionally resulting with breaking the Pwnix operating system.
- All "*One-Touch*" applications should be closed "gracefully" using CTRL+C whenever possible. This can be performed by first pressing and releasing the **Volume Down** button, followed by tapping the letter "**C"** on the terminal keyboard.
- Only one directly attached external, USB adapter is supported for use at a time. To attach multiple external USB adapters simultaneously, an externally powered USB hub is required, though a non-powered hub may support up to two devices at a time depending on power draw of the connected adapters.
- The device's internal wireless and Bluetooth hardware does **not** support packet injection or monitor mode. While it may be possible to use other adapters, the included external USB wireless and Bluetooth adapters are the recommend adapters for use with the Pwn Pad 3.

Basic Navigation

All basic navigation uses the front-end Android 4.4.2 Kit Kat operating system. Swiping, tapping, and tap-and-hold are all part of Android's native navigation system.

Closing apps: To close an app, tap the multi-view (i.e. the double rectangle icon) in the bottom right hand corner. Then, from the app window list, swipe an app window off the screen and to the right to close the app. See the screenshot to the right.

Multi-view can also be very useful for switching between apps (equivalent to ALT+TAB on a desktop/laptop computer).

Connecting to Wi-Fi Networks

Swipe down from top right corner of the screen and select 'Wi-Fi'. Next, swipe Wi-Fi from OFF to ON, wait a few seconds then select the network to connect to from the list of visible access points.

Note: For hidden networks tap the + button in the upper right hand corner and type in network name and select security type to enter password, tap 'Save'.

Important: After connecting to an available access point, the first thing before using the Pwn Pad is to update it and afterward, restart it. Please refer to the next section entitled, "*Updating the Pwn Pad*".

Updating the Pwn Pad 

Updates to the Pwnix operating system are made available every 4-6 weeks while updates to the underlying applications themselves available from Kali occur almost daily. Keeping both Pwnix and Kali up-to-date is easy. Just open the Admin tools folder and run the "Update" application.

When the "Update" application is launched, the current Pwnix release installed is displayed on the screen. Type '1' to begin the process of downloading and installing all available updates. After the process has finished, the current Pwnix release installed is displayed on the screen. Next, exit the Terminal window by tapping "X" in the upper right corner, then restart the Pwn Pad.

IMPORTANT: Always reboot (i.e. restart) the Pwn Pad 3 after installing updates.

Note: If a proxy server is required for connectivity to the Internet, the update process will not be successful. Please ensure there is an exclusion to allow the Pwn Pad to bypass the need of using a proxy server. Else, connect the Pwn Pad to a wireless network that does not require the use of a proxy server.

Troubleshooting Tip: If the update process indicates a failure, open the "Root Shell" application in the Admin tools folder and type the command below followed by pressing Enter. Afterward, exit "Root Shell", then run the "Update" application, also in the Admin tools folder.

```
# rm –f /opt/pwnix/chef/latest-version-id
```

If the update process still indicates a failure, please review the */var/log/pwnix/update.log* file for possible connectivity issues. Please note updates are retrieved using TCP port 443 from the web sites listed below. In some networks using web-filtering solutions, it may be necessary to add/create exclusions to allow access to these web sites, then remove the */opt/pwnix/chef/latest-version-id* file and update again.

updates.pwnieexpress.com
kalirepo.pxinfra.net
gemrepo.pxinfra.net

Update Notifications

To ensure the Pwn Pad is always up-to-date it, it is recommended to enable the "*Update Notification*" option. After enabling this feature and should an update become available for Pwnix, a notification prompt will appear at the top of the screen.

Note: The Update Notifications feature requires Google Play Services, including Google Play Store. Neither of which are installed on the Pwn Pad by default. When enabling the "Update Notifications" option, Google Play Services, including Google Play Store will be installed and available for use.

Perform the following steps to enable "Update Notifications", which will additionally install Google Play Services, including Google Play Store.

1. Enable the built-in wireless adapter and connect to an access point to establish connectivity to the Internet.
2. Next, open the Admin Tools folder and run the "Pwnix Express Updates" application.
3. Enable the checkbox for the "Receive Update Notifications" option.
4. When prompted to install "Google Play Services", select "Yes".
5. After the download has completed, swipe downward from the top of the screen and tap on "Services download complete" to begin the process of installing the application(s).
6. When prompted, select "Yes" to install and reboot the Pwn Pad.
7. After rebooting, the Pwn Pad is available for use.

   At this time, the process to enable "*Update Notifications*" is complete. In addition, the Google Play Services and Google Play Store applications are now installed and available for use on the Pwn Pad.

Connecting External Adapters

All USB adapters included with the Pwn Pad should be connected using the provided MicroUSB OTG cable and attached using Velcro to the back of the case.

Included USB adapters will show up as the following interfaces in the Kali chroot environment:

- The *TP-Link High Gain 802.11a/b/g/n 150MBps Wireless adapter* is used with WiFi related applications including, Kismet, WiFite, EvilAP, etc. The adapter will appear as **wlan1**. And after an application is launched in association with this adapter, it will additionally appear as **wlan0mon** and/or **at0**.

  Note: If booting with TP-Link Wi-Fi adapter attached, please allow 30 seconds after boot before attempting its use with any application

- The *SENA Bluetooth adapter* is used with Bluetooth related applications, including BlueLog, BlueScannr, RedFang, HCITool, etc. The adapter will appears as **hci0**.

- The *TrendNet USB-Ethernet adapter* is used to connect the Pwn Pad to a wired network. The adapter will appear as **eth0.**

One-Touch Applications

The Pwn Pad 3 provides five folders (Admin, Network, Wireless, Attack and Bluetooth) organizing the "One-Touch" applications by type. The first application in each folder is the icon used to display the folder.

Note: Many of the 'Network', 'Wireless', and 'Attack' tools can be used together simultaneously to perform different discovery and pen-testing tasks. Many tools have the ability to run on any desired interface and may be used to layer attacks and tools on a single interface at once.

For example, initially launch the One Touch EvilAP application to create a fake access point, then launch the One Touch Nmap application, selecting the "at0" interface to scan for live targets having connected to network created by the fake access point

IMPORTANT: A majority of "One-Touch" Applications provide an opportunity to choose to save files pertaining to the data captured when using the application. By default, all capture files are stored to the 'Captures' directory (i.e. */opt/pwnix/captures*) and the respectively named subdirectories below.

For example:

/opt/pwnix/captures/
/opt/pwnix/captures/nmap
/opt/pwnix/captures/
/opt/pwnix/captures/
/opt/pwnix/captures/
etc.

Admin Tools folder 

The Admin Tools folder provides shortcuts to applications useful for the administration and maintenance of the Pwn Pad, including updating the Pwn Pad, copying (arching) captures files, and deleting log files.

Captures Dump

This application will copy the 'Captures' directory (i.e. */opt/pwnix/captures/) and all subdirectories* to an attached USB drive using the USB OTG cable.

Note: The USB drive must be formatted FAT32 and connected before running this application.

Factory Reset

This application will restore the Pwn Pad to its original default image when shipped. After performing a Factory Reset, it will be necessary to run the "Update" application to bring the Pwn Pad up-to-date with the current release of Pwnix and Kali tools. Please refer to the section entitled, "*Updating the Pwn Pad*".

WARNING: Performing a Factory Reset will **DELETE ALL DATA** on the Pwn Pad itself though the SD card may still contain files. If necessary, run the "*Captures Dump*" application beforehand.

IMPORTANT: Do **not** use the Factory Data Reset feature available within Android Settings. Doing so will cause the Pwn Pad to revert to an Android 4.4.2 stock image, additionally resulting with breaking the Pwnix operating system.

Log Wiper

This application will securely wipe the 'Captures' directory and all subdirectories, as well as all system logs, tmp files, and/or bash history if desired. If necessary, run the "*Captures Dump*" application beforehand.

Pwnie UI On/Off

This application will either enable or disable the local Pwnie web-based UI. For the mobile product line, the Pwnie UI is primarily used for configuring reverse shells (see "Using the Reverse Shells").

When the Pwnie web-based UI is enabled use a web browser on a laptop/desktop system in the same network and connect to https:///*[device_ip_address]*:1443

Alternatively, you can launch the web browser application on the Pwn Pad itself and connect to https://127.0.0.1:1443

Note: The default username and password to access the Pwnie web-based UI (or SSH server) is: **pwnie : pwnplug8000**

Important: Be sure to change the password for the "pwnie" user account before using the Pwn Pad in an untrusted environment. To do so, either log into the Pwnie web-based UI and select "Authentication" found on the Settings page, or login to the Pwn Pad using SSH (see "SSH On/Off") and run the following command:

```
$ passwd
```


Root Shell

This application provides Kali chroot environment access via Android Terminal Emulator.

Using the "Root Shell" application provides the ability to run Debian Linux commands as well as any of the 100+ installed applications and packages from a terminal session.

SSH On/Off

This application will either enable or disable the SSH server on the Pwn Pad.

Alternatively, users may open the "Root Shell" application and type:

 # service ssh start

When the SSH Server is started you can SSH directly into the Pwn Pad from a Linux/Mac computer on the same network, as shown:

user@linux/mac_computer$ **ssh pwnie@*ip_address_of_device***

Note: The default username and password to access the SSH server (or the Pwnie web-based UI) is: **pwnie : pwnplug8000**

Important: Be sure to change the password for the "pwnie" user account before using the Pwn Pad in an untrusted environment. To do so, either login to the SSH server and run the following command, or log into the Pwnie web-based UI and select "Authentication" found on the Settings page.

$ passwd

IMPORTANT: The "pwnie" user account is a standard user with sudo privileges. Most of the system commands and pen-testing tools referenced in this manual must be run as root, as indicated by a hash tag (#) proceeding a command. Once logged in as "pwnie", you can sudo to root as follows:

$ sudo su

Update

This application will update your Pwn Pad to the latest Pwnix software release, as well as update any Kali applications installed. Internet connectivity is required.

IMPORTANT: The update process will reset certain system config files in */etc and /opt/pwnix* to their default state. If you have manually customized configuration files in these locations, be sure to back them up any before updating the device, else any changes made will be overwritten.

Troubleshooting Tip: If the update process indicates a failure, open the "Root Shell" application in the Admin tools folder and type the command below followed by pressing Enter. Afterward, exit "Root Shell", then run the "Update" application, also in the Admin tools folder.

 # rm –f /opt/pwnix/chef/latest-version-id

If the update process still indicates a failure, please review the output displayed for possible connectivity issues. Please note updates are retrieved using TCP port 443 from the web sites listed below. In some networks using web-filtering solutions, it may be necessary to add/create exclusions to allow access to these web sites.

updates.pwnieexpress.com
kalirepo.pxinfra.net
gemrepo.pxinfra.net

Network tools folder 

The Network Tools folder provides shortcuts to applications commonly used in association with wired and wireless networks, including traffic sniffers, etc.

Dsniff

This application displays clear text usernames and passwords in transit on the selected interface, with an option to log to */opt/pwnix/captures/passwords/*

For further information visit http://www.monkey.org/~dugsong/dsniff/

MAC Changer

This application will randomize the MAC address and hostname of the selected interface.

Hint: In an unknown wired network where an IDS/IPS may be in use, it may be beneficial to use this application *before* running Nmap.

For further information,, visit https://github.com/alobbs/macchanger

Nmap

This application will quickly identify live hosts on the network associated with the selected interface, as well as identify the open ports/services for each host.

Note: The underlying method used is to perform a ping sweep for host discovery against the local subnet (/24), with an option to subsequently run service detection. All scan output is saved to */opt/pwnix/captures/nmap_scans/*

Hint: For persons familiar with the use of Nmap and the different switches it provides, it may be preferred to run Nmap from a Root Shell. Simply open the "Root Shell" application, then type **nmap** and press Enter for a list of available switches.

For further information, visit http://nmap.org/book/man.html

Strings Watch

This application written by Pwnie Express and based on will shows human readable strings in the network traffic passing through the selected interface, with an option to log to the */opt/pwnix/captures/stringswatch/* directory.

TCPdump

This application will display raw network traffic on the selected interface, with an option to capture all results to */opt/pwnix/captures/tcpdump/*

For further information, visit http://www.tcpdump.org/

Tshark

This application will display network traffic via the command-line version of Wireshark, with an option to log to */opt/pwnix/captures/tshark/.*

Hint: For persons familiar with the use of Tshark and the different switches it provides, it may be preferred to run Tshark from a Root Shell. Simply open the "Root Shell" application, then type **tshark –-help** and press Enter for a list of available switches.

For further information, visit https://www.wireshark.org/docs/man-pages/tshark.html

Wireless tools folder 

The Wireless Tools folder provides shortcuts to applications used to perform discovery and testing of access points on wireless networks.

Airodump

This application will display all in-range wireless APs and client devices in real time, including probe requests from clients. An pption to save captures to /opt/pwnix/captures/wireless/ is additionally provided.

Note: GPS logging is now supported! To log wireless networks with GPS location data simply enable GPS device (either through Settings>Location Access>ON or via the device quick launch widget bar on the home screen) then wait for it to acquire a lock by observing the GPS icon in upper right hand corner (will become solid once GPS position is acquired). Next, open and minimize the 'BlueNMEA' application. Afterward, open the Airodump application, which will automatically detect the 'BlueNMEA' app running and start logging with the GPS.

Important: Always use the '**Volume Down**' button and 'C' key to close this app gracefully before disconnecting the wireless adapter!

For further information, visit http://www.aircrack-ng.org/doku.php?id=airodump-ng

Kismet

This application will log all in-range wireless devices and data traffic (packets). After launching, press "Tab", then "Enter", then press the "down arrow" in bottom left hand corner to minimize the on-screen keyboard.

Note: GPS logging is now supported! To log wireless networks with GPS location data simply enable GPS device (either through Settings>Location Access>ON or via the device quick launch widget bar on the home screen) then wait for it to acquire a lock by observing the GPS icon in upper right hand corner (will become solid once GPS position is acquired).

Next, open and minimize the 'BlueNMEA' application. Afterward, open the Kismet application, which will automatically detect the 'BlueNMEA' app running and start logging with the GPS.

For further information, visit https://www.kismetwireless.net/

WiFite

This application provides an automated wireless attack / auditing tool using the Aircrack-NG suite. After launching, the display will sort AP's by signal strength and automatically refresh the display every five seconds. When it's desired to begin an attack, press the 'Volume Down' button and 'C' to lock the display and to select a target(s).

Note: Always use the 'Volume Down' button and 'C' key to close this app gracefully before disconnecting the wireless adapter!

For further information, visit https://code.google.com/p/wifite/

Attack tools folder 

The Attack Tools folder provides shortcuts to applications that can be used to initiate attacks and perform penetration testing upon wired and wireless networks.

DNS Spoof

Note: The EvilAP app must be running before launching this tool.

This application is used in combination with EvilAP or Social Engineering Toolkit (website cloner), redirecting all outbound DNS requests to the IP address of the local EvilAP (IP 192.168.7.1).

For further information, visit http://www.monkey.org/~dugsong/dsniff/

Ettercap

This application serves as a "*Man-in-the-Middle*" (MiTM) tool suite to perform ARP cache poisoning with known target IP addresses, additionally providing an option to log to */opt/pwnix/captures/ettercap/*

For further information, visit https://ettercap.github.io/ettercap/

EvilAP

Aggressive wireless access point used to forcefully associate wireless clients in range with using the client's preferred network list. Select internet connection (wlan0 if connected to wifi), select channel, choose SSID network name to broadcast, enable probes or not. **Note:** Always use the 'Volume Down' button and 'C' key to close this app gracefully before disconnecting the wireless adapter!

For further information, visit https://www.pwnieexpress.com/introduction-evilap/

For a practical example of using EvilAP, see https://www.pwnieexpress.com/evilap-practical-example/

Metasploit

This application is used to run MSF Console (msfconsole) offered within the latest stable release of the Metasploit Framework.

For further information, visit https://www.metasploit.com/

In addition, visit https://www.offensive-security.com/metasploit-unleashed/msfconsole/

SET aka "Social Engineering Toolkit"

This application is used to run the Social Engineering Toolkit (SET), which can be used for "*Man-in-the-Middle*" (MITM) attacks combined with social engineering.

For further information, visit https://www.trustedsec.com/social-engineer-toolkit/

In addition, visit http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/

SSL Strip

This application will attempt to "*strip*" SSL encryption from certain connections by serving HTTP-only versions of requested URLs on the selected interface.

Note: Many modern web browsers (i.e. Chrome, Firefox, etc.) are no longer susceptible to this form of attack, often the result of the browser using a plug-in (i.e. "*HTTPS Everywhere*", etc.) or the web server implementing HSTS.

For further information, visit http://www.thoughtcrime.org/software/sslstrip/

In addition, visit https://github.com/LeonardoNve/sslstrip2

Bluetooth Tools folder 

The Bluetooth Tools folder provides shortcuts to applications used to oerform the discovery and capture traffic in association with Bluetooth devices.

Bluelog

This application scans for Bluetooth devices in the attempt to "pair" with another device or broadcasting its presence. Automatically creates a log file, reflecting the device name, MAC address, and class id to */opt/pwnix/captures/bluetooth/*

For further information, visit http://www.digifail.com/software/bluelog.shtml

Bluetooth Scan

This application scans for Bluetooth devices using 'hcitool -i hci0 scan --flush --class --info' showing detailed Bluetooth data about each device found, including device type, class, and services available. Automatically creates a log file to */opt/pwnix/captures/bluetooth/*

For further information, visit http://linux.die.net/man/1/hcitool

Ubertooth

This application provides three applications, to be used to capture full-packet Bluetooth traffic using the Ubertooth tool suite.

Note: To use this application, an UbertoothOne adapter **is** required. This adapter is **not** included with the purchase with the Pwn Pad, but may be obtained from http://ubertooth.sourceforge.net/

Using the tools

Airodump

Airodump can be used to quickly view in a real time all wireless (802.11) access points and wireless clients in a given area. If logging is enabled it will save multiple capture file types to */opt/pwnix/captures/wireless*.

When opening Airodump enter '**1**' to log captures (if desired). Once Airodump has placed the wlan1 interface (TP-Link WiFi adapter) into monitor mode (creates mon0 interface) it will automatically start channel hopping all channels and displaying wireless APs and Clients. To sort by various views (i.e. sort by beacons, signal strength, channel, encryption, etc.) press '**s**' on the on screen keyboard to cycle through each view. Press '**TAB**' to highlight APs and clients connected.

Airodump Sorting View:

Landscape Mode:

NOTE: If the 'Manufacturers' are not displaying any known vendors, it means the oui.txt file is not present or out of date. Simply connect to a wireless network with Internet access and open Airodump again and it will automatically download and use an updated oui.txt file.

To force an update to the manufacturer's list file, run the following command from a Root Shell with Internet access:

airodump-ng-oui-update

Airodump Unassociated Client Probe Request:

Exiting Airodump:

Kismet

Kismet is a great tool for wireless sniffing and unlike Airodump is less real time oriented with a more collective layout of devices and wireless events seen. Everything Kismet "sees" will be viewable in the interface. This becomes useful when collecting wireless packet captures to check for specific devices, with the ability to view device details even after a device is no longer active or out of range. Kismet is also a great tool for saving multiple types of capture files and mapping networks with a GPS. To use Kismet with the GPS, simply perform the GPS steps above prior to opening Kismet. GPS coordinates will show up once the internal GPS has a signal lock. Significant improvements have been made to the Kismet UI for customs views, displaying detailed information about network and client details. To use the Pwnie custom UI configuration file, be sure to update the device to the latest release, and open a root shell and run:

rm -r /root/.kismet/

Once the '/root/.kismet/' folder is removed; the Pwnie custom UI configuration file will be copied there from '/etc/kismet/kismet_ui.conf'. The Kismet UI may then be customized as necessary and can be restored to the custom Pwnie UI configuration by removing the '/root/.kismet/' folder again.

When opening Kismet with the Pwnie configuration file, the user will only have to hit 'Enter' key once to have Kismet up and fully operational. Use the arrow keys to navigate up and down networks seen. In the second window below networks seen is a list of clients connected to the current selected network. Use the 'TAB' key to navigate between networks and clients. Use the 'Enter' key to view further details of a selected network or client. To navigate the Kismet menu use the 'ESC' key and arrow keys.

NOTE: Curses has some screen drawing display issues, turning the screen sidewise into landscape mode should reset and redraw the interface. Hitting 'ESC' and opening menus will also redraw the screen if needed. This can be avoiding by keeping the on-screen keyboard up as well.

NOTE: Be SURE to close Kismet with 'Volume Down' button + 'C' to gracefully exit. This will remove wlan1mon interface that Kismet creates which otherwise will stay present and can cause the device to reboot if the TP-Link adapter is removed!

Opening Kismet First Screen:

Main Screen User Interface:

Kismet Clients Window:

Kismet Landscape View:

EvilAP

The EvilAP has many useful security applications, from both a pen-testing perspective as well as using it to spot check wireless devices in an environment. There are two main modes of running the EvilAP - aggressive mode (responding to probe requests from wireless clients) and static mode (acting purely as an access point without forcing wireless clients to connect). Both modes can be useful in different scenarios, one thing to note is that Airbase-ng can get overloaded easily when trying to respond to too many probe requests in aggressive mode, and will sometimes crash. Aggressive mode is most useful when checking to see if any clients in proximity are automatically connecting to open networks. Clients within range that have open networks in their preferred network list set to "connect to when available" will automatically connect to the EvilAP thinking it is a network previous connected to. The same thing will occur in static mode if the SSID of the EvilAP matches and open network in the wireless clients preferred network list. This is important to note when pen-testing and targeting specific wireless clients because once the client connects in aggressive mode the user then knows the SSID the client is connecting to and can re-run the EvilAP in static mode with the target client's preferred SSID. Running in static mode is more stable in general and is more reliable for performing scans and attacks layered on top of the EvilAP.

Spot-checking an environment for this vulnerability is the best use case when not performing a pentest, and can be helpful for security admins to walk around their environment and ensure there are no company devices automatically connecting to open networks when they should not be. Network printers are a perfect example of this, because often when configuring them people forget to disable the wireless interface altogether.

When opening the EvilAP, first select the interface that will be supply Internet access. Unless there is an active SIM card in the device, most likely the source of Internet access will be the internal wireless card (wlan0).

NOTE: The internal wireless card (wlan0) if connected to a wireless network will block the internal 4G GSM card, only select the GSM interface if the device is not connected to a wireless network via wlan0 interface and there is an active SIM card present in the device. The same is true for connecting the Ethernet adapter (eth0); the internal wireless card (wlan0) will always take routing priority over other interfaces available when connected.

Once the Internet source interface is chosen, enter an SSID (wireless network name). If planning to run in aggressive mode, this will not matter so much as the EvilAP will broadcast all SSIDs, cycling through probe requests seen from wireless clients.

If planning to run in aggressive mode, select '**1. Yes**' for responding to probe requests. The default value beacon rate for broadcasting probes is 30 milliseconds, with a range of 20-70. The default will work in most cases, but if clients are connecting and dropping this is a value that can be adjusted to achieve a more reliable connection from clients.

EvilAP MiTM attack in aggressive mode with SSLStrip, Strings Watch and Dsniff:

This implementation provides a demonstration of the HTTPS stripping attacks presented at Black Hat DC 2009. It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial. For more information on the attack, see the video available at https://vimeo.com/50018478

Below is an example of running a fake access point to trick wireless clients into automatically connecting to the device with the *EvilAP*. *SSLStrip* is then run on top of the *EvilAP* (at0) interface to provide clients with HTTP versions of HTTPS secure websites. Other tools can be layered on top such as *Strings Watch* and *Dsniff* to monitor relevant traffic and credentials from the client in a human readable format. All tools can log to the captures folder located at */opt/pwnix/captures/*.

Open 'EvilAP' from 'Wireless Tools'

First, establish and verify connectivity to the Internet using the built-in wireless adapter. Next, follow the step by step instructions below:

1. Launch EvilAP and select the adapter providing connectivity to the Internet (e.g. internal wireless card wlan0) 	2. Enter the SSID to spoof (i.e. attwifi or linksys, netgear, xfininitywifi, etc.) 
3. Enter Channel to use (1 is default - hit enter or select different channel if 1 is in use	4. Enter '1. Yes', to broadcast wireless client probe requests, i.e. use "*Karma Attack*". Else, enter '2. No', to host an access point

to avoid interference) 	using the SSID specified. 
5. If Karma Attack is used, hit 'Enter' for default beacon rate (increase or decrease value if clients have trouble connecting). 	6. Observe client device establishing connection to the EvilAP. 

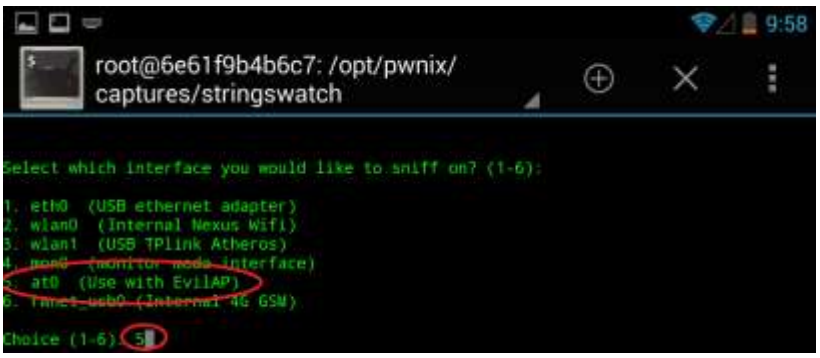
7. Next, go to Home screen to launch 'SSLStrip' from 'Attack Tools', then select interface to sniff on (EvilAP interface is at0) 	

Open 'SSLStrip' from 'Attack Tools'

1. Select interface to sniff on (EvilAP interface is at0)
2. Hit home screen to launch 'Strings Watch' from 'Network Tools'

Open 'Strings Watch' from 'Network Tools'

1. Select interface to sniff on (EvilAP interface is at0)
2. Choose to log or not
3. Hit home screen to launch 'Dsniff' from 'Network Tools'



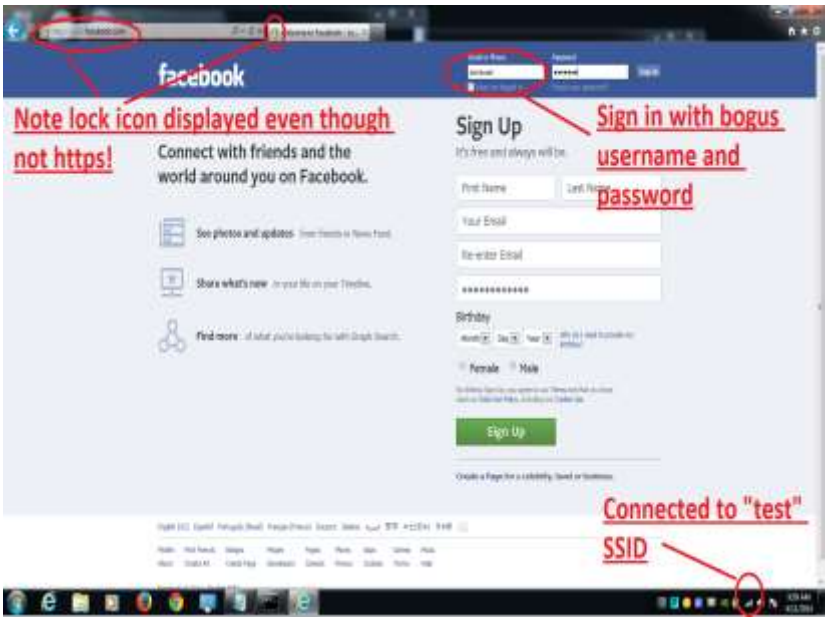
Open 'Dsniff' from 'Network Tools'

1. Select interface to sniff on (EvilAP interface is at0)
2. Choose to log or not

User may now swipe across terminal screens with finger to view output from each tool and monitor traffic and any credentials sniffed.

On Windows 7, target wireless client connected

In the example, the target wireless client is a Windows 7 user browsing to facebook.com. In the example the user is logging in with bogus credentials to show the password can be sniffed because the web session in HTTP and not HTTPS, meaning the user's traffic is all in clear text and viewable from the device.



On the device:

Swipe across each terminal window to see traffic and credentials sniffed.

Strings Watch output:

Dsniff output:

When finished swipe back to the EvilAP window and gracefully close the EvilAP by pressing the 'Volume Down' button on the right side of the device and the 'C' key on the on screen keyboard. This will restore the original hostname and MAC address the gets rolled randomly when the EvilAP is started.

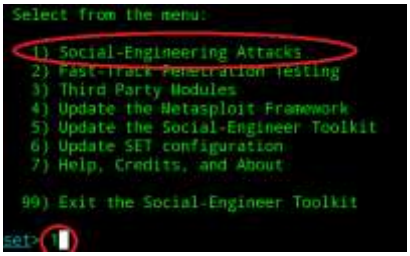
EvilAP MITM + DNS spoofing + fake login page with the Social Engineering Toolkit + Dsniff:

Running the EvilAP can be combined with many different types of MITM attacks. Another good example of one is using the 'DNS spoof' app with 'SET' on top of the running EvilAP. The Social Engineering Toolkit is an extensive suite providing many types of attacks. One of the easiest most effective attacks to setup with SET is the website cloning attack. Using SET, the pen tester can clone the login page of any desired website, and have the fake page hosted from the device. Then using DNS spoof, all DNS requests from connected wireless clients will be required to the fake login page running on the EvilAP. This essentially turns the EvilAP into a captive portal like the way a public hotspot works initially when a client connects and has to login. Because SET hosts an HTTP version of the cloned login page, any credentials entered will be in clear text and therefore easy to sniff.

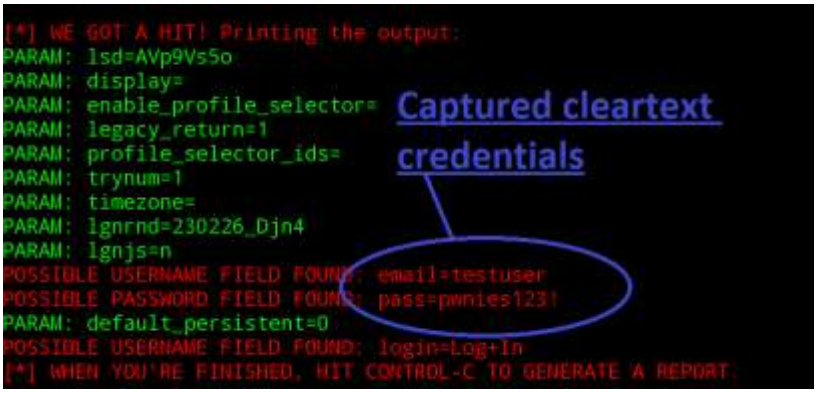
Open 'EvilAP' app from the 'Wireless Tools' menu and run as desired given the example in the previous attack above, then go back to the home screen.

Open 'SET' app from the 'Attack Tools' menu and enter the following selections to setup a cloned login page:

1. 1 (Social-Engineering Attacks)
2. 2 (Website Attack Vectors)
3. 3 (Credential Harvester Attack Method)
4. 2 (Site Cloner)
5. 192.168.7.1 (Address of the EvilAP - to host the fake login page on)
6. facebook.com (Address of website login page to clone)
7. Hit the home screen icon



Once wireless client attempts to login to fake website login, credentials will be displayed in the SET window



Open 'DNS Spoof' from the 'Wireless Tools' menu (NOTE: Currently only works when EvilAP is already running). Once running go back to the home screen.

Open 'Dsniff' from the 'Network Tools' menu

1. Select interface to sniff on (EvilAP interface is at0)
2. Choose to log or not

Even though SET already shows you the credentials once the wireless client attempts to login, Dsniff can be useful to have running as well to see the IP address of wireless clients as they connect. Dsniff output will also show DNS requests being made, and of course, any clear text credentials captured.

Everything can be closed gracefully using 'Volume Down' button and 'C' as stated in the previous example.

Additional command-line pen-testing tools

Thanks to the rock stars at the Kali Linux project (kali.org), all below pen-testing tools are pre-installed as Debian packages and can be run from any path in the Kali chroot environment:

aircrack-ng	gpsd	p0f	Sslstrip
amap	grabber	pingtunnel	Stunnel
arp-scan	hping3	plecost	Tcpflow
arping	httptunnel	proxychains	thc-ipv6
Bed	hydra	proxytunnel	theharvester
bluelog	iodine	redfang	Tinyproxy
bluez	john	scapy	Ubertooth

cisco-auditing-tool	kismet	setoolkit	Udptunnel
cisco-global-exploiter	lbd	sendEmail	ussp-push
cryptcat	mdk3	sipcrack	Waffit
darkstat	metagoofil	sipsak	Wapiti
dmitry	miranda	skipfish	Weevely
dns2tcp	miredo	smtp-user-enum	Wepbuster
dnsenum	nbtscan	snmpcheck	Wifitap
dnstracer	netcat	socat	Wifite
dsniff	netdiscover	sqlmap	xprobe2
ettercap	ngrep	sqlninja	Reaver
fierce	nikto	ssldump	Bully
fimap	nmap	sslscan	OpenVAS
Fping	onesixtyone	sslsniff	

Pentesting Resources

Provided below are a few recommended resources.

Kali Linux Tools Listing:
http://tools.kali.org/tools-listing

PTES Technical Guidelines:
http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Metasploit Unleashed:
http://www.offensive-security.com/metasploit-unleashed/Main_Page

Hacking Exposed Wireless, 3rd Edition; Wireless Security Secrets & Solutions
http://www.amazon.com/Hacking-Exposed-Wireless-Third-Edition/dp/0071827633

Packt Publishing:
https://www.packtpub.com/networking-and-servers?search=kali

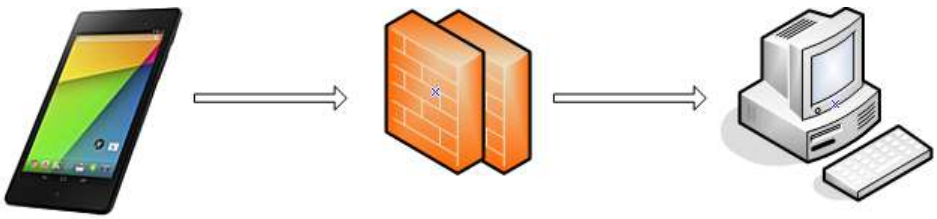
Using the reverse shells

Overview

- All Pwnie devices include aggressive reverse tunneling capabilities for persistent remote SSH access.
- SSH over HTTP, HTTPS/SSL, DNS, ICMP, and other covert tunneling options are available for traversing strict firewall rules, web filters, & application-aware IPS.
- All tunnels are encrypted via SSH and will maintain access wherever the device has an Internet connection - including wired, wireless, and 4G/GSM where available.

Typical Deployment

1. On a staging/lab network, enable the desired reverse shells (see "Activating the reverse shells")
2. Configure a Kali Linux system to receive the reverse shells (see "Configuring Kali to receive the reverse shells")
3. Test the reverse shells in a lab / local LAN to confirm all shells are working as expected (see "Connecting to the reverse shells")
4. Deploy the device to your target network and watch your SSH receiver for incoming shells (see "Deploying to target network")



Pwnie device on target network

Firewall on target network

SSH Receiver (Kali)

Activating the Reverse Shells

For the Pwnie Express mobile product line (Pwn Pad, Pwn Phone, etc.), the Pwnie UI is used for configuring the reverse shells.

1. To enable the Pwnie UI, touch the 'PwnieUIonOff' button on the home screen:

NOTE: Currently SSHD must be running for shells to work!

Pwnie UI On/Off

2. Open a web browser and access the Pwnie UI: https://*[device_ip_address]*:1443
3. The UI is SSL-enabled, but you will receive a warning as the certificate is self-signed.
4. At the login prompt, enter your username/password (default is **pwnie : pwnplug8000**)
5. The "Setup" page appears.

   IMPORTANT: Be sure to change the default "pwnie" user password as soon as possible. This password can be changed in the Pwnie UI under "System Authentication". This will change the password for the 'pwnie' UI user and the 'pwnie' SSH user account.

6. Click "Reverse Shells" on the top menu.
7. Click the name of the shell you wish to configure.

   Tip: To best maintain persistent remote access, enable all of the reverse shells. Enter the SSH shell receiver IP address or DNS name for each selected reverse shell. The device will connect to this shell receiver system to establish the reverse shell connections.

8. Choose how often the reverse shell connection should be attempted. By default, a shell connection will be attempted every minute (recommended).

   Tip: To use an HTTP proxy for the "SSH over HTTP Tunnel", enable the "Use HTTP Proxy" checkbox and enter the proxy server address and port (and optionally, proxy server credentials).

   Note: The HTTP proxy auth password is stored in clear text in /opt/pwnix/pwnix-scripts/script_configs

9. Click "Configure" to apply your changes for the reverse shell you're configuring.

   Note: The following SSH client config directives (/etc/ssh/ssh_config) are set on all devices to allow for automation of reverse shell connections. Be sure you understand

the security implications of these settings before connecting to other SSH servers from the device.

```
StrictHostKeyChecking no
UserKnownHostsFile /dev/null
```

10. Proceed to configure Kali to receive the reverse shells.

Configuring Kali to Receive Reverse Shells

A Kali Linux system (Kali Linux 1.0.6 or later) can serve as the SSH tunnel "receiver". Your Pwnie device will connect to this system when initiating the reverse shell connections.

Note: These steps assume you're using Kali Linux 1.0.6as your SSH receiver. Older Kali distributions may be used, but different steps may apply.

1. Place your Pwnie device and the Kali system on the same local network/subnet
2. Login to the Kali system and open Firefox
3. Connect to the UI: https://*[device_ip_address]*:1443
4. Login to the UI when prompted.
5. Click "Reverse Shells" on the top menu.
6. Click the "Download Shell Receiver script for Kali Linux" link at the top of the page (under step 5) to download the "pwnix_ssh_receiver.sh" script.
7. Save the script file (pwnix_ssh_receiver.sh) into the user's home directory (selected by default)
8. Open a terminal window and enter the following commands:

```
# cd
# chmod +x pwnix_ssh_receiver.sh
# sudo ./pwnix_ssh_receiver.sh
```

9. The script auto-configures and starts the reverse shell listeners on Kali.
10. When prompted, enter the desired certificate information for the stunnel SSL certificate (or just press ENTER to accept the defaults)
11. Once the auto-config script completes you will see:

```
[+] Setup Complete.
[+] Press ENTER to listen for incoming connections..
```


12. Press ENTER to watch for incoming device connections. Each reverse shell will attempt to connect using the interval you specified in the UI.

    Tip: You can list all active device connections at any time by typing:

    ```
    # netstat -lntup4 | grep 333
    ```

13. Proceed to "Connecting to the reverse shells".

Connecting to the Reverse Shells

NOTE: The SSH service must be running at least locally on the device in order to connect to reverse shells.

1. Open a terminal window on your Kali shell receiver system and connect to any available "listening" Pwnie device shell as follows:
    - **Standard SSH:** ssh pwnie@localhost -p 3333
    - **SSH Egress Buster:** ssh pwnie@localhost -p 3334
    - **SSH over DNS:** ssh pwnie@localhost -p 3335
    - **SSH over SSL:** ssh pwnie@localhost -p 3336
1. Enter your Pwnie device's "pwnie" user password and voila! You're now remotely connected to the device through the reverse shell.
2. Proceed to "Deploying to target network"

    Standard SSH / SSH Egress Buster Note: If there's no firewall between your Pwnie device and your shell receiver system, be sure the shell receiver system SSH server is listening on the ports you selected for the Standard Reverse SSH and SSH Egress Buster shells in the UI. For example, if you set port 31337 for Standard Reverse SSH, add the line "Port 31337" to /etc/ssh/sshd_config, then restart SSHd (/etc/init.d/ssh restart).

    Tip: The SSH receiver address can be anonymized using the "Tor Hidden Service" feature as described here http://www.securitygeneration.com/security/reverse-ssh-over-tor-on-the-pwnie-express/

    Special thanks to Sebastien J. of Security Generation for streamlining the SSH receiver setup process, and to Lance Honer for his resilient autossh script improvements.

Deploying to Target Network

1. Place your shell receiver system behind a public-facing firewall.
2. Configure the appropriate port forwarders on your firewall:

- **Standard Reverse SSH:**
  Forward the port selected in the UI to port 22 of your shell receiver.
- **SSH over SSL:**
  Forward port 443 to port 443 of your shell receiver system
- **SSH over DNS:**
  Forward UDP port 53 to UDP port 53 of your shell receiver system
- **SSH Egress Buster:**
  Forward all ports selected in the UI to port 22 of your shell receiver system

1. In the Pwnix UI ("Reverse Shells" page), configure the reverse shells to connect to your firewall's public IP address (or DNS name if available).
2. You can now deploy your Pwnie device to your target network. The device will automatically "phone home" to your shell receiver system, providing encrypted remote access to your target network.

   Tip: In some environments, you may wish to schedule a nightly reboot of the device to re-initiate all connections from the device side. This way, if some part of the connection process crashes on the device side (for example, sshd), the connection process will start "fresh" again after the reboot.

Maintaining your Pwn Pad

Reviewing the Pwnix environment

The following commands run from within a Root Shell can be helpful.

Show device software revision:
 # grep Release /etc/motd

Show kernel version:
 # uname –r

Show current date/time:
 # date

Show file system disk usage (note your disk usage may vary):
 # df –h

Show CPU details:
 # cat /proc/cpuinfo

Show total memory:
 # grep MemTotal /proc/meminfo

Show current eth0 config:
 # ifconfig eth0

Show currently listening TCP/UDP services (note dhclient won't be present if not using DHCP):
 # netstat –lntup

Check syslog for errors, warnings, etc:
 # egrep -i "warn|fail|crit|error|bad|unable" /var/log/messages

Show Ruby version:
 # ruby –v

Show Perl version:
 # perl –v

Show Python version:
 # python –V

Factory Reset feature

The 'Factory Reset' application in the Admin Tools folder will perform a complete restore of the Pwn Pad to the image that was flashed on the device when it was shipped. This feature is a "One-Touch" application making the restore process easier than ever allowing the user to do a full restore without re-flashing the device from a computer. No internet connection or computer is required with the process being performed entirely from the device itself!

Important: Always backup any data desired to be saved before doing a factory reset! Also note that files in /sdcard/ may NOT get wiped.

Transferring files to/from your device

Transferring files via ADB commands

Note: These steps require 'android-adb-tools' to be installed on a Linux host computer:

1. Attach the device to a Linux computer with ADB tools installed.

2. Open a root shell on the Linux computer and change directory to the desired location to receive files to:

   user@linuxcomputer$ **mkdir captures**
   user@linuxcomputer$ **cd captures/**
   user@linuxcomputer$ **adb shell**
   shell@deb:/ $ **su**

root@deb:/ # **bootpwn**
root@localhost:/# **cd /opt/pwnix**
root@localhost:/# **cp -a captures/ /sdcard/**
root@localhost:/# **exit**
root@deb:/ # **exit**
shell@deb:/ $ **exit**
user@linuxcomputer$/ **adb pull /sdcard/captures/**

3. To remove temporary captures folder from /sdcard:

   user@linuxcomputer$/ **adb shell**
   shell@deb:/ $ **su**
   root@deb:/ # **rm -r /sdcard/captures/**

Note: This method will only pull folders with files in them, and not empty directories

Transferring Files via SCP

Note: Using scp does not require having to copy the captures folder to /sdcard/.

1. Enable the device's local SSH server (see "Remote terminal via SSH").
2. From a Linux host computer connected to the same local network:

   user@linuxcomputer$ **scp -r**
   pwnie@*ip_address_of_device***:/opt/pwnix/captures/ .**

How to Obtain Support

All Pwn products come with FREE technical support during the first thirty-days from the initial date of purchase. After thirty-days, the ability to obtain technical support requires a subscription to "*Pwnie Care*".

- *What is the URL to the Support Center or to read product-related support articles?*

  The Support Center is available at http://support.pwnieexpress.com

- *What is the URL to the Support Portal?*

  The Pwnie Express Support Portal is available at http://www.pwnieexpress.com/pages/support

- *What is the URL to visit the Support Forum?*

  The Pwnie Express Support Forum is available at http://forum.pwnieexpress.com

- *What is the email address to submit technical support requests?*

  You can submit an email to request support via the Support Portal at http://support.pwnieexpress.com/customer/portal/emails/new or you can send an email to support@pwnieexpress.com

- *What is the phone number to call to request technical support?*

  Call our main number at 855-793-1337, then select option 3

Command Terminals

Local Terminal Emulator

Android Terminal Emulator is the local terminal application, used by one-touch pen-testing apps to open a root shell into the Kali Linux chroot environment and run tool scripts.

Each time a one-touch pen-testing app is launched it will open Android Terminal Emulator, spawn a shell in the Kali chroot environment, then run the underlying script specific for that tool.

To open a root shell within the Kali chroot environment, simply touch the 'Root Shell' icon on the home screen. The root shell will start in the */opt/pwnix/captures/* directory.

NOTE: To select, copy and paste within the terminal tap and hold the screen until a menu pops up. Tap 'Select' and then carefully underline desired text to select with finger. Once selection has been made remove finger from the screen, tap and hold on screen again until menu pops up, select 'Paste' to paste in copied selection.

NOTE: To move between different terminal windows, simply swipe with finger in each direction left to right or right to left.

Tethered Terminal via USB cable

USB debugging mode (enabled by default) allows direct command terminal access to your device from a Linux host computer over USB.

To proceed, "android-adb-tools" must be installed on your Linux host computer. To install android-adb-tools on an Ubuntu 12.04 system:

```
user@linuxcomputer# sudo add-apt-repository ppa:nilarimogard/webupd8
user@linuxcomputer# sudo apt-get update
user@linuxcomputer# sudo apt-get install android-tools-adb
```

Once android-adb-tools is installed, attach the device to your Linux host computer using the manufacturer supplied Micro USB to USB cable. A few seconds after connecting the device to the Linux host computer, the device should prompt to "Allow USB debugging" with an RSA key associated with the host computer. Click "OK" to continue.

Next, on your Linux host computer enter the following commands to access the device's Kali chroot environment:

```
user@linuxcomputer$ adb shell
shell@deb:/ $  su
root@deb:/ #  bootpwn
[+] Mounting filesystems…
[+] Filesystems mounted.
[!] Welcome to the Pwn zone. Get your game face on.
root@localhost:/#
```

